

- (e) logic defining an interface usable to interact with a user and to control playback of said audiovisual content.
- 3. (previously presented) The medium of claim 2 further comprising program logic for an interpreter of a Turing-complete language, where:
  - (i) said program logic is configured to perform a plurality of security checks; and
  - (ii) said program logic is configured to permit playback of said audiovisual content provided that said security checks are successful.
- 4. (previously presented) The medium of claim 3 where said program logic is configured to invoke at least one cryptographic operation supported by at least one of said authorized playback devices.
- 5. (previously presented) The medium of claim 3 where said program logic is configured to perform at least one operation necessary for decryption of said audiovisual content by at least one said authorized playback device.
- 6. (previously presented) The medium of claim 2 wherein a subset of said authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and further comprising program logic which, when executed by a device of each said vulnerable model, is configured to:
  - (a) mitigate said vulnerability affecting said vulnerable playback device; and
  - (b) perform at least one operation necessary for said vulnerable playback device to decrypt said audiovisual content.
- 7. (previously presented) The medium of claim 6 where said program logic includes executable code for a Turing-complete virtual machine.

8. (previously presented) The medium of claim 6 where said operation necessary to decrypt includes updating a cryptographic key contained in said playback device.
9. (previously presented) The medium of claim 6 where said program logic for mitigating includes native executable code configured to detect whether the security of a vulnerable device has been compromised.
10. (previously presented) The medium of claim 6 where said program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device.
11. (previously presented) The medium of claim 6 where said program logic for mitigating includes a firmware upgrade for correcting at least one vulnerability.
12. (previously presented) A device for securely playing digital audiovisual content, said audiovisual content including a plurality of regions each having multiple versions thereof, comprising:
  - (a) a media drive including a laser for use in reading data from rotating optical media;
  - (b) a nonvolatile memory containing:
    - (i) a set of cryptographic player keys for use with a broadcast encryption system, and
    - (ii) identifiers of revoked media;
  - (c) a bulk decryption module for decrypting encrypted audiovisual content from said media;
  - (d) program logic configured to:
    - (i) select a version of each said region;

- (ii) decrypt said selected version, whereby a combination of said versions selected in the course of playing said media uniquely identifies said device;
- (e) at least one codec for decompressing said audiovisual content; and
- (f) media verification logic configured to verify:
  - (i) whether valid digital signatures contained on said media authenticate said media, and
  - (ii) whether said media are identified as revoked in said nonvolatile memory.
- 13. (previously presented) The device of claim 12 further comprising an interpreter for a Turing-complete language, where said interpreter is configured to obtain said program logic from said drive and execute said program logic.
- 14. (previously presented) The device of claim 12 further comprising means for reducing the output quality of said audiovisual content if a security requirement specified by said medium for high-quality output is not met.
- 15. (previously presented) The device of claim 12 wherein:
  - (a) said combination of versions selected during the course of playback of any one said medium uniquely does not uniquely identify said playback device; and
  - (b) said combination of versions selected during the course of playback of a plurality of said media does uniquely identify said playback device.
- 16. (previously presented) A method for playing encrypted digital audiovisual content from a digital medium, comprising:
  - (a) verifying a digital signature authenticating said medium;
  - (b) retrieving at least one player key from a nonvolatile memory;

- (c) using said at least one player key with a broadcast encryption system;
  - (d) using a result of said broadcast encryption system to decrypt at least a portion of said audiovisual content;
  - (e) reading program logic for a Turing-complete interpreted language from said optical medium;
  - (f) using an interpreter to execute said program logic, where said interpreter performs operations specified in said program logic to respond to selections from a user;
  - (g) selecting a variant from a plurality of variants for each of a plurality of portions of said audiovisual content, where:
    - (i) said player is capable of decrypting said selected variant; and
    - (ii) said player lacks at least one cryptographic key required to decrypt at least one non-selected variant for each said portion; and
  - (h) decrypting each said selected variant.
17. (previously presented) The method of claim 16 where said user selections include button presses on a remote control.
18. (previously presented) The method of claim 16 where said program logic directs said player to perform an AES block cipher operation via said interpreter.